The True Cost of Downtime:

A 7-Part Strategy for Protecting Your Practice

There's one thing that healthcare administrators want more than anything else when it comes to IT. They want to work so they don't have to worry about it.

It doesn't seem like too much to ask, but one thing is as certain as sickness itself. No matter how well managed they are, IT systems will, at some point, fail.

That being the case, the most important question healthcare administrators can ask is, "How do I avoid downtime when a failure occurs?"

In fact, beyond IT concerns, "How do I avoid downtime?" is one of the most important questions to address for your entire healthcare organization. The costs of downtime are devastating and, in some ways, incalculable.

The Direct Costs of Downtime

Downtime immediately sets off a cascade of costs that are visible and measurable.

1. **Staff Struggles to Serve Patients Effectively –** From long wait times and missed appointments to the lack of data necessary for a diagnosis, downtime leaves your staff unable to properly care for the people who need you.
2. **Patients Suffer Injury –** In 2017, a statistic was revealed through For the Record magazine that 70% of hospitals had seen one or more patients injured during downtime.
3. **Lost Revenue and Productivity –** Both Everbridge, an emergency communications management firm, and the Poneman Research Institute have confirmed that downtime in a hospital easily can easily exceed $8,500 per minute.
4. **Technological Costs –** Downtime can lead to data loss, errors, or the unthinkable – a security breach which creates its own secondary cascade of costs and potential HIPAA penalties.

The Indirect Costs of Downtime

What's even worse, difficult to see, and perhaps impossible to calculate are these further costs of downtime.

1. **Loss of Trust –** When IT systems fail, a natural customer response is to question the competency of the practice. After all, "If they can't keep their business running, how can I expect them to keep me running?"
2. **Damage to Your Reputation –** Whether it's through word-of-mouth, negative online reviews, or critical patient experience surveys, there's almost no way to manage the groundswell of dissatisfaction that downtime can trigger.

Avoid Downtime by Implementing an Agile, Fault-Tolerant Infrastructure

The path to preventing downtime begins by anticipating a system failure and architecting an environment that minimizes its impact to your medical practice.

Practices with several locations in the same geographic area are uniquely able to mitigate IT system and facilities downtime. By designing their business processes and IT systems to be agile, these practices can:

- React to failures and reallocate resources quickly
- Continue to care for patients even if an entire site is taken offline

When the right system is in place, your staff can transition from "fire-fighting reaction mode" to making fast, strategic decisions based on existing contingency plans. You can ensure continuity of service for your patients and productivity for your staff.

Why Don't More Healthcare Organizations Do This?

Given those benefits above, it's surprising that more healthcare organizations fail to implement an agile infrastructure. There are at least three formidable obstacles holding them back.

1. **Cost –** The cost and effort to implement an agile, fault-tolerant IT infrastructure can be significant. Because of that, these projects aren't usually prioritized until a major failure causes a business interruption. By that time, it's clear that the costly fallout detailed above eclipses the costs of prevention.
2. **Risk –** Many administrators would rather stick with the imperfect solution they know rather than risk further damage by making a change.
3. **Lack of a Dependable IT Partner –** It's even harder to take a risk if you lack confidence in your IT partner, and far too many healthcare businesses have found it hard to find an IT provider they can trust to manage the complexities and unique challenges of healthcare.

Here's What We've Learned by Focusing Solely on Healthcare IT

PEAKE Technology Partners has a focus that is rare among IT providers. Healthcare is all we do, and below is what we've learned over the years by partnering with healthcare providers to solve the unique challenges that face your industry.

This 7-part strategy will empower you to build the agile, fault-tolerant infrastructure you need to avoid downtime and protect your patients and practice.

1 Rank Your Systems

First, we need to understand which systems are essential to your practice's operations.

Fault tolerance gives a system the ability to continue functioning after a component failure. However, it's costly to implement, and it's prudent to identify which IT systems and business processes are truly mission critical.

- Some choices are obvious. EMR, telephones, and patient check-in systems are all essential.
- Others fall into a grey area. What would happen if ePrescribe or faxing was unavailable for a day? What about printing?

Develop a list of all IT and facility systems that are used by the practice, then rank each system on a priority scale of 1 to 3:

- P1 systems are mission critical
- P2 systems would cause a major process interruption
- P3 systems are for convenience.

Here's an example list:

System	Priority
Electronic Healthcare Records	P1
Centralized Telephone System	P1
eFax	P2
Waiting Room WiFi	P3
Automated Patient Check-in	P2
Prescription Printers	P2
ePrescribe Interface	P2
Public Website	P2
Individual Location Power / Connectivity	P2
Digital Signage	P3

For each P1 system, fault tolerance is required.

For P2 systems, a cost/benefit analysis should be performed to determine if the cost of service interruption is outweighed by the cost of protection. In performing the analysis, remember to consider customer loss and employee productivity.

Generally, fault tolerance is not needed for P3 systems. With a list of critical systems in hand, the next step is to develop plans to protect each one. This is a task that requires close collaboration between the practice management team, the IT team, and the facilities team.

For each critical IT system, a plan must be developed to ensure that the system is fault-tolerant by always being:

1. Available
2. Functional
3. Accessible

2 Protect the Availability of Your Systems

For an IT system to be available, its underlying hardware and software must be fault-tolerant. This means removing single points of failure in each system layer, from power and cooling to processing and storage. Several approaches can achieve this result:

1. **Cloud Service Providers –** The most straightforward method involves outsourcing the entire application to a cloud service provider. In this case, the vendor is responsible for delivering a fault-tolerant environment and provides a service level agreement describing its availability guarantee.
2. **Hybrid Approach –** Another approach involves outsourcing a portion of the environment, usually the expensive-to-build "hosted computing" layer, and maintaining private control and management of the application itself. This approach can yield cost savings and flexibility benefits when compared to a cloud service provider, but it requires a highly-skilled IT team to execute successfully.
3. **In-House –** The third approach involves building the necessary fault-tolerant systems in-house and maintaining them privately. Generally, this approach is only cost effective for the largest private practices.

Each approach will, if implemented properly, provide the same result. Failures within customer facilities, telecommunication carrier networks, electric utilities, or IT hardware systems will no longer affect availability of the core application used within your critical system.

3 Protect the Functionality of Your Systems

IT system functionality describes the ability of the system to fulfill its users' needs. Although a system may be available from a technical sense, if it is not behaving as intended, it will not satisfy business requirements.

- Vendor support agreements which feature a guaranteed response time are an effective way to ensure system functionality.
- In addition, the IT team must be trained and ready to quickly engage multiple vendor resources when complex problems arise.
- A centralized help desk that coordinates multiple support resources is essential. A seamless support framework must exist within the practice to connect users with the correct support teams when issues arise.

4 Protect the Accessibility of Your System

Accessibility defines whether authorized users can access a particular resource. Even if an IT system has 100% availability from an application perspective, if its users cannot reach the system due to a telecommunications failure at an individual practice location, the business requirement will not be served.

The prevention of accessibility issues is usually handled in two ways:

- First, connectivity technologies should be chosen with reliability in mind. Fiber-based data circuits, for example, are generally more reliable than coaxial cable-based data circuits. Likewise, enterprise-grade connections with a service level agreement provide higher uptime than consumer-grade connections.
- Second, multiple circuit technologies can be combined to provide fault tolerance using a feature set known as SD-WAN. This provides a seamless failover experience if one circuit suffers an outage. (It's important to note, however, that although two different service providers may be available at a particular location, they may both share physical network assets, and may therefore be vulnerable to common failure modes.)

5 Develop Business Processes for Continuity

Identifying and protecting mission-critical systems is an essential step toward developing fault tolerance in a private medical practice, but the business continuity journey doesn't end there. Business processes must also be developed and maintained in order to adapt to other failures.

Although careful planning and system building can ensure that P1 systems remain available, functional, and accessible, special business processes must be developed, documented, and tested on a regular basis to adapt to P2 and P3 failures.

Using the list of system priorities developed earlier, identify systems that are not protected from failure through fault tolerance at the system level, and develop a continuity plan that copes with unavailability of the individual system.

For example, power failure at an individual practice location requires a plan detailing how to temporarily relocate employees to another location, communicate the change to patients with scheduled appointments, report the power outage to building management, and so forth.

While developing these business continuity processes, be sure to use multiple physical locations to your advantage. For example, a group of spare workstations at a well-placed practice location could serve as a disaster recovery site for the patient scheduling center or billing group.

Finally, as business processes are developed, they must be effectively documented and communicated to relevant employees on a continuing basis. Continuity plans are only effective if they're regularly updated to reflect changes in business practices and personnel.

6 Perform Failure Testing

Regardless of the rigor applied during the planning process, new considerations will always arise when a failure occurs in practice. Testing and simulation exercises allow us to account for this reality.

Failure testing, of course, can be disruptive, so careful planning is again required to expose process flaws while minimizing operational disruption. Here are some best practices you can follow:

- Failure testing of fault-tolerant P1 systems can be performed by the IT operations team during maintenance windows.
- Drills for failures that involve employee response and contingency plan activation can be scheduled during known low-patient-volume periods.
- Simulated failure procedures should be designed with a rapid rollback plan in place, so that normal operations can be resumed if a flaw in the documented recovery plan is exposed.

Finally, testing activities should be repeated on a regular basis and the results documented for future reference.

7 Find an IT Partner You Can Trust

For most organizations, healthcare IT is too complex to manage in-house. Regardless, any organization will benefit from the guidance of a reliable IT partner who has shepherded other businesses through the transition to fault-tolerant systems.

However, any healthcare administrator can tell you how \ difficult it can be to find an IT partner who can handle the unique challenges of healthcare.

That's why this is all we do, and it's why we've built an army of experts in healthcare IT to support you. We share your concern for your patients, and we understand how critical it is to avoid even a minute of downtime.

We understand that in healthcare IT, the most important thing is trust.

- PEAKE Technology Partners gives you 99.99% Uptime Reliability.
- In addition to that army we mentioned, we've built our own data center to make sure it happens.
- To ensure your security, we also built our own private internet network.

Our focus and dedication to healthcare has earned a 97% Customer Retention Rate, and we stand ready to serve you as well.

Here's How We Partner with You

Schedule a Consultation

We'll make sure we understand the unique needs of your medical business, and we'll build a custom solution that supports them.

Make a Smooth Transition

The most intimidating part of any change in IT partners is the handoff. We'll make sure it runs smoothly with minimal disruption for your team.

Have a Partner You Can Trust

Trust is earned, and we'll be working 24/7 to make sure you have secure Healthcare IT that runs reliably in the background of your busy day.

You can avoid the devastating costs of downtime and instead have a partner you can trust in protecting continuity of service for your patients and productivity for your staff.

Let's work together.

SCHEDULE A CONSULTATION

PEAKEtechnology.com | 1-866-357-3253

PEAKE™ TECHNOLOGY PARTNERS